NASUNI®

Ransomware Recovery in the 'New Normal'

Nasuni's Shaw and Bilotti on How to Prepare, Respond and Share Files Securely

iSMG
INFORMATION SECURITY
MEDIA GROUP

David Shaw

John Bilotti

The ransomware threat has scaled up to match the new remote workforce. But have backup policies and incident recovery procedures improved to keep pace? **David Shaw** and **John Bilotti** of Nasuni share tips on ransomware recovery, remote file-sharing and business continuity.

In an interview with Tom Field of Information Security Media Group, Shaw and Bilotti discuss:

- Ransomware recovery challenges;
- Securing a remote file-sharing environment;
- Business continuity successes in crisis response.

The primary architect of Nasuni's cloud NAS, Shaw is an acknowledged expert on the security of file systems who holds numerous patents for distributed data storage and other disciplines. As chief science officer, he oversees Nasuni's efforts to develop security innovations while complementing the efforts of the office of the CTO. Shaw joined Nasuni in 2009 after holding development positions at Hitachi Data Systems and Archivas.

Bilotti is a network support and IT veteran with over 25 years of experience in technology. As Nasuni's CIO, he oversees corporate IT, business applications, information security and data privacy. Bilotti holds numerous industry credentials, including Certified Information Security Manager (CISM) from ISACA. He joined Nasuni as a senior leader for its customer support department in 2015 and went on to further develop Nasuni's information security and compliance program.

The Recovery Challenges

TOM FIELD: Why is it so hard to recover from a ransomware attack even though companies practice good backup policies?

DAVID SHAW: A ransomware attack is incredibly disruptive. The companies need to prevent further harm, figure out how the infection happened and see if they can prevent it from happening again. Once you're back up again, you don't want to leave something latent on your network that could put you right back where you started.

A good backup is great and crucial, but you also need to figure out which backup to use. The backup has to be from before the infection, so you need to know exactly when the original infection happened. Plus, in some cases, your backup could be reachable over the network, and ransomware increasingly is trying to seek out those backups and encrypt them along with your original files. A lot of details have to be worked out.

JOHN BILOTTI: In contrast, if you're following these standards and your backups are off-site, you then have a lot of time to obtain those backups, get them either shipped in or gain access to them remotely, and figure out what it's going to take to restore that all when your IT resources are also trying to deal with containing the ransomware attack and make sure it's not spreading further and other issues that might be coming up as part of the incident.

SHAW: Right. So there's a lot of stuff to work out. It's not something that an IT department, even the best IT department, is going to knock it out in an afternoon.

An Evolving Threat

FIELD: Talk to me about how the ransomware threat has changed now that we've got almost all of our workers working remotely.

BILOTTI: The biggest concern with a remote workforce, regardless of the industry that you're in, is your workers are working from their home environment on networks that you as an IT organization don't have a lot of control over. A lot of times, they're sharing those network resources with children and siblings and using them for recreational activities other than just business.

The fear is you can't control the network in the traditional sense. So you need to be prepared for ways to get visibility into what might be happening that could potentially, especially with regard to ransomware, get back into a ransom attack on company data when they're connected in through their VPN and attaching to file shares. I think that's the thing that makes it challenging, with that combined workload.

SHAW: I would expect to see an uptick in the coming weeks of the number of infections reported due to people working at home as a result of COVID-19. There are a lot of personal machines being used, and they're not getting that locked down in protected environments that are usually put in place by corporate IT.

BILOTTI: Related to the world events with the pandemic, more and more individuals are seeking information. So they're visiting websites that are advertising charts and graphs and statistics and active world events. Unfortunately, there are people out there who are adversaries who are also creating fictitious or malicious sites related to that. So we're seeing an uptick in phishing attempts, in gathering attempts, raising that threat of something like malicious code or ransomware because people are visiting things they normally don't, and they're leveraging that change in work habits or behaviors.

Nasuni's Role

FIELD: David, let's talk a little bit about Nasuni in terms of the issues we're having with the ransomware threat. How do you offer ransomware recovery to your customers?

SHAW: We offer a fast file recovery. What makes it fast is, there's a rewiring of the file rather than a slow copy of the file. You want to rewire any files in need of replacement when recovering from ransomware. This could be because someone deleted it, or it could be because ransomware encrypted it. Either way, you're going to want your files back.

Now, because Nasuni's gold copy of the file system is in the cloud, rolling a file back to early state, that's basically replacing the bad file or missing file with a pointer to an earlier version of the file. And because the gold copy is incremental, there's an earlier version to get back to.

> "The biggest concern with a remote workforce is your workers are working from their home environment on networks that you as an IT organization don't have a lot of control over."
>
> John Bilotti, Nasuni

So you have a file system that's correct for the current time, and you're moving that moment in time for that particular file or series of files to a point in the past, because we're continually versioning this. You can likely find a version that was captured ideally as soon as possible before the infection.

It's important to understand that this isn't sequential. We can restore individual files, or we can restore full volumes on as many files at the same time, so the cloud can ship all of that at once.

> “I’m glad we had a continuity plan that we had put in place and previously tested and discussed with our executives.”
>
> John Bilotti, Nasuni

Selecting a Vendor

FIELD: What types of security should companies look for in their remote file-sharing environments?

BILOTTI: When you’re selecting a vendor, you want to make sure that their security program takes into account industry best practices, such as end-to-end encryption, and allows you as a company to use secure keys and hold and manage those keys yourself so they’re not off with a third party. You want to make sure that if you are putting your data in the cloud, you’re not compromising on the security you would have if it was in your own corporate enterprise. You want to take those standards and extend them to a remote workforce and to remote file-sharing, and ensure that you select somebody that gives you that robust environment to continue with your access controls and your user access provisioning necessary to meet your needs.

Business Continuity

FIELD: We all saw the world change pretty dramatically just a few weeks ago with the advent of the pandemic and the remote workforce. What parts of the Nasuni business continuity plan are you glad you had in place when the world changed?

BILOTTI: I’m glad we had a continuity plan that we had put in place and previously tested and discussed with our executives. Nasuni is lucky enough to be a software company where we’re able to make remote transition relatively easy and continue doing what we do as a corporation, where that may not be true in other industries where they’re producing or manufacturing goods.

Very early in our company history, we had decided since we were a cloud-native service offering, that it was very important in the design of what we do and how we operate that we’re not dependent on any particular physical office or lab or data infrastructure. We wanted to leverage the tools and technologies available to us, leveraging the cloud to be able to support a remote workforce regardless of what the world conditions are.

Our business continuity plan was based on the fact that we could, with very little fail-over effort, swap over to a 100% percent remote workforce. One-third of our workforce already is remote. We’re based out of Boston, and we’ve got sales and marketing and support people all over the United States and the world, and they’re working remotely full-time already.

So it wasn’t a huge transition, but we were happy that we had everything in place to support that remote effort. It was much more than just having good network connectivity. It was having proper communication tools in place and methods to share information from remote file-sharing, having web-based, knowledge-based articles that are cloud hosted that people can get into and get information.

So just being able to have everybody continue with the day-to-day activity and working and collaborating even though they’re not sitting in a physical office together was key.

SHAW: With the various groups I’m working with for the upcoming version of our product, we’ve been using our own tools for file-sharing to transport information around. We’re using Slack and Zoom like much of the rest of the world is right now. Working from home has been actually quite effective. ■

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANKiNFO SECURITY® CUiNFO SECURITY® Just for Credit Unions GOViNFO SECURITY® HEALTHCAREiNFO SECURITY®

iinfoRisk® TODAY CAREERSiNFO SECURITY® Data Breach. Prevention. Response. Notification. TODAY CyberEd.io

iSMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io